А. С. Бестужев

Вятский государственный гуманитарный университет,
schools@chgk43.ru

О СТРОЕНИИ КОНЕЧНЫХ ЦИКЛИЧЕСКИХ ПОЛУКОЛЕЦ

Введем определения. *Полукольцом* называется алгебраическая структура $\langle S, +, \cdot, 0, 1\rangle$, в которой $\langle S, +, 0\rangle$ — коммутативный моноид, $\langle S, \cdot, 1\rangle$ — полугруппа, выполняются законы дистрибутивности операции умножения относительно сложения, тождественно $0 \cdot s = s \cdot 0 = 0$ для всех $s \in S$. *(Мультипликативно) циклическим полукольцом* называется полукольцо, все элементы которого, кроме нуля и единицы, являются натуральными степенями некоторого элемента a ($a \neq 0$, $a \neq 1$), нуль же может являться, а может и не являться степенью элемента a; считаем, что $a^0 = 1$.

Строение бесконечных циклических полуколец известно и определяется законами сложения: $a^m + a^n = a^{\min\{m,n\}}$ или $a^m + a^n = a^{\max\{m,n\}}$. В дальнейшем рассматриваются только конечные циклические полукольца.

Возможны два случая:

1) одна из степеней элемента a равна нулю;

2) среди степеней элемента a нет нуля.

Рассмотрим первый случай: $a^n = 0$, где n — минимальная степень элемента a, такая, что $a^n = 0$. Тогда $1, a, a^2, \ldots, a^n$ — попарно различны. Строение таких полуколец определяет

Теорема 1. *Если в циклическом полукольце нуль является степенью образующей a, то $a^m + a^n = a^{\min\{m,n\}}$.*

Рассмотрим второй случай, когда нуль не является степенью образующей. Строение таких полуколец помогает выяснить

Теорема 2. *Если в циклическом полукольце нуль не является степенью образующей, и сумма двух различных элементов равна нулю, то данное полукольцо является полем.*

Далее, обозначим через s сумму $s = 1+a+a^2+a^3+\dots+a^{n-1}$. Возможны два случая:

1) $s = 0$;

2) $s \neq 0$.

Опираясь на теорему 2, для первого случая можно доказать, что полукольцо является конечным полем.

Второй случай: $s \neq 0$. В данном случае полукольцо будет устроено так: элементы $1, a, a^2, a^3, \dots, a^{k-1}, a^k$ — различные, причем $a^k = a^{k+1}$. В дальнейшем будем рассматривать только такие полукольца, а элемент a^k будем всегда называть поглощающим, так как a^k в произведении с любым элементом дает a^k.

Предложение. *Сумма $1+a^k$, где a^k — поглощающий элемент, может принимать одно из двух значений 1 или a^k.*

Рассмотрим первый случай: $1 + a^k = 1$. Домножим равенство $1 + a^k = 1$ на a^n: $a^n + a^k = a^n$. В этом случае сумма любого элемента с a^k дает этот же самый элемент. Нетрудно понять, что в множестве $S\backslash\{0\}$ поглощающий элемент играет роль нуля — при умножении на поглощающий получаем поглощающий, а при сложении с поглощающим получаем тот же самый элемент. Получаем, что $S\backslash\{0\}$ — циклическое полукольцо, в котором нулевой элемент является степенью образующей.

Строение таких полуколец нам известно. Само полукольцо S получается присоединением к полукольцу $S\setminus\{0\}$ нуля.

Второй случай: $1 + a^k = a^k$. Домножим это равенство на a^n: $a^n + a^k = a^k$. Это значит, что поглощающий по умножению элемент будет еще и поглощающим по сложению. Среди таких полуколец существуют идемпотентные, в которых $1 + 1 = 1$, и неидемпотентные, в которых $1 + 1 = a^m$, где $m > 0$. Аддитивная полугруппа циклических идемпотентных полуколец является верхней полурешеткой. Дальше будут рассматриваться только неидемпотентные циклические полукольца $S = \{1, a, a^2, \dots, a^k, 0\}$, где $a^k = a^{k+1}$, поглощающий элемент всегда будем обозначать a^k. Чтобы задать полугруппу по сложению для такого полукольца, достаточно задать суммы единиц со всеми элементами, оставшиеся суммы находятся по свойству дистрибутивности. Введем новые обозначения. Запись $a^{3,4}$ означает, что на месте $a^{3,4}$ может стоять как элемент a^3, так и элемент a^4; выражение $a^{3,\dots,7}$ значит, что на его месте может находиться любой из элементов a^3, a^4, a^5, a^6 или a^7. Например, равенство $1 + a = a^{3,4}$ говорит о том, что сумма $1 + a$ может быть равна a^3 или a^4. А запись $a^{3,\dots,7} + a^{3,\dots,7} = a^{7,\dots,10}$ означает, что все суммы $a^3 + a^3, a^3 + a^4, \dots$ $\dots, a^3 + a^7, a^4 + a^4, \dots, a^7 + a^7$ равны любому из значений a^7, a^8, a^9, a^{10} (каждая сумма принимает любое из этих значений). В дальнейшем будем использовать следующую классификацию полуколец. Предположим, что в полукольце не все суммы равны поглощающему элементу. Тогда найдется такое число n, что $a^{0,\dots,k} + a^{n+1,\dots,k} = a^k$, и не все суммы с элементом a^n равны поглощающему элементу. По свойству дистрибутивности, все суммы с элементом a^n равны a^{k-1} или a^k.

Найдется такое число m, что $a^{m+1,\ldots,k} + a^n = a^k$ и $a^m + a^n = a^{k-1}$. Ясно, что $m \leqslant n$. Можно сказать так, что мы хотим провести классификацию полуколец по первой "непоглощающей" сумме "сверху".

Введем новые обозначения. Пусть у нас есть полукольцо с поглощающим элементом a^k, где $k = m + n + p + 1$. Поясним, что за числа m, n, p. Это такие числа, что в полукольце выполняются равенства (*): $a^{0,\ldots,k} + a^{m+n+1,\ldots,k} = a^{m+1,\ldots,k} + a^{m+n} = a^k$ и $a^m + a^{m+n} = a^{m+n+p}$.

Свойство. *Если в полукольце выполняются равенства* (*), *то* $p > m$.

Теорема 3. *Возможен один из следующих четырех случаев:*

1) $n - 1 < m$;
2) $n - 1 \geqslant m,\ p > n - 1$;
3) $n - 1 \geqslant m,\ p \leqslant n - 1,\ 1 + 1 = a^{n+1,\ldots,k}$;
4) $n - 1 \geqslant m,\ n - 1 \geqslant p + m,\ 1 + 1 = a^n$.

Для первых трех случаев получены формулы, описывающие строение всех таких полуколец, которые не представлены в данной статье.

Перечислим суммы элементов с единицей для четвертого случая. Заметим, что не все структуры, соответствующие перечисленным случаям, будут являться полукольцами, но все возможные полукольца представлены. Итак:

$$1 + a^k = \cdots = 1 + a^{m+n+1} = a^k,\ 1 + a^{m+n} = a^{k-1,k},$$
$$1 + a^{m+n-1} = a^{k-2,k-1,k}, \ldots, 1 + a^{n+1} = a^{n+p+1,\ldots,k},$$
$$1 + a^n = a^{n+p},\ 1 + a^{n-1} = a^{n+p,\ldots,k},$$
$$1 + a^{n-r} = a^{m+n+1,\ldots,k}\ (r = p - m), \ldots,$$
$$1 + a^{m+1} = a^{m+n+1,\ldots,k},$$
$$1 + a^m = a^{m+n,\ldots,k},\ \ldots,\ 1 + 1 = a^n.$$

Здесь следует обратить внимание на то, что в правой части равенства не может появиться элемент a^{m+n}, пока показатель степени у второго слагаемого в левой части больше, чем m.

Для четвертого случая приведем пример, как устроены полукольца, взяв конкретные значения чисел m, n, p, k, а именно, $m = 1$, $n = 4$, $p = 2$, $k = 8$. Все структуры, согласно приведенным выше общим формулам, определяются так:

$$1 + a^{6,7,8} = a^8,\quad 1 + a^5 = a^{7,8},\quad 1 + a^4 = a^6,\quad 1 + a^3 = a^{6,7,8},$$
$$1 + a^2 = a^{6,7,8},\quad 1 + a = a^{5,6,7,8},\quad 1 + 1 = a^4.$$

Среди них полукольцами будут только следующие структуры:

$$1 + a^{6,7,8} = a^8,\quad 1 + a^5 = a^7,\quad 1 + a^4 = a^6,\quad 1 + a^3 = a^6,$$
$$1 + a^2 = a^{6,7,8},\quad 1 + a = a^5,\quad 1 + 1 = a^4;$$

и

$$1 + a^{6,7,8} = a^8,\quad 1 + a^5 = a^8,\quad 1 + a^4 = a^6,\quad 1 + a^3 = a^{7,8};$$
$$1 + a^2 = a^{6,7,8},\quad 1 + a = a^{6,7,8},\quad 1 + 1 = a^4.$$